AO 106 (Rev. 04/010) Application for Search Warrant AUTHORIZED AND APPROVED/DATE: Tiffany Edgmon 4/22/24

UNITED STATES DISTRICT COURT

for the

WESTERN DISTRICT OF OKLAHOMA

In the Matter of the Search of)
)
Toyota Sienna bearing Mexico) Case No: M-24-364-STE
license plate XAJ-659-B and VIN)
TDYK3DC6DS333454)

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

See Attachment A, which is attached and incorporated by reference.

FILED
APR 22 2024
CARMELITA REEDER SHINN, CLERK
U.S. DIST. COURT, WESTERN DIS. OKLA.
BY DEPUTY

Located in the Western District of Oklahoma, there is now concealed:

See Attachment B, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim.P.41(c) is (*check one or more*):

- ☒ evidence of the crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2422(b)	Attempted Coercion or Enticement of a Minor
18 U.S.C. § 2423(b)	Interstate Travel with Intent to Engage in a Sexual Act with a Minor
18 U.S.C. § 2252A(a)(5)(B)	Possession of Child Pornography

The application is based on these facts:

See attached Affidavit of Special Agent Andrea Salazar, Homeland Security Investigations, which is incorporated by reference herein.

- ☒ Continued on the attached sheet(s).
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).

Applicant's signature

Andrea Salazar
Special Agent
Homeland Security Investigations

Sworn to before me and signed in my presence.

Date: April 22, 2024

Judge's signature

City and State: Oklahoma City, Oklahoma

SHON T. ERWIN, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent Andrea Salazar, with Homeland Security Investigations, am being first duly sworn, state as follows:

INTRODUCTION

1. I am currently employed as a Special Agent ("SA") with Homeland Security Investigations ("HSI") and have been so since July 2022. Prior, I was a federal police officer with Pentagon Force Protection Agency and had been so employed since August 2019. I hold a bachelor's degree in criminology and a Master of Public Administration from St. Mary's University. I also hold a Master of Science in Criminal Justice from Sam Houston State University.

2. I am currently assigned to HSI Office of the Resident Agent in Charge Oklahoma City, Oklahoma. As part of my various duties and responsibilities, I investigate federal criminal cybercrime violations. As it relates to cybercrime, I have gained experience conducting child exploitation and child pornography investigations. My working experience has been augmented by training I received at the Federal Law Enforcement Training Center. Moreover, I have access to the institutional knowledge developed around this type of investigation by working with other experienced child exploitation criminal investigators. I have become aware of numerous examples of child pornography. Additionally, I have had the opportunity to observe and review hundreds of images and videos of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. Moreover, I am a federal law enforcement officer who

is engaged in enforcing criminal laws, including 18 U.S.C. § 2422(b) and 2423(b).

3. I am investigating the online activities of Bryan Devin CRUZ ("CRUZ"). As explained herein, there is probable cause to believe CRUZ committed the following crimes: Attempted Coercion and Enticement of a Minor, in violation of 18 U.S.C. § 2422(b); Interstate Travel with the Intent to Engage in a Sexual Act with a Minor, in violation of 18 U.S.C. § 2423(b); and Possession of Child Pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B).

4. I submit this Application and Affidavit in support of a search warrant authorizing a search of the **SUBJECT VEHICLE**, as further described in Attachment A. Located within the **SUBJECT VEHICLE**, I seek to seize evidence, fruits, and instrumentalities of the foregoing criminal violations, as further described in Attachment B.

5. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the foregoing violations are presently located at the **SUBJECT VEHICLE**.

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a

format that resembles an oral conversation. This feature distinguishes chatting from other text based online communications such as Internet forums and email.

b. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

c. "Child Sexual Abuse Material" includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

d. "Computer" refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." *See* 18 U.S.C. § 1030(e)(1).

e. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives,

floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

f. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alphanumeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

g. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

h. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer

software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

i. "Minor" means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).

j. "Sexually explicit conduct" applies to visual depictions that involve the use of a minor, see 18 U.S.C. Section 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, see 18 U.S.C. Section 2256 (8)(C). In those contexts, the term refers to actual or simulated (a) sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person. *See* U.S.C. § 2256(2)(A).

k. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

l. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact

discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

m. A "storage medium" or "storage device" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

n. A "website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as HyperText Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text transport Protocol (HTTP).

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

7. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or

she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

8. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child sexual abuse material where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software,

which may have been used to create the data (whether stored on hard drives or on external media).

9. Furthermore, I know that modern tablets (a type of "computer," as broadly defined in 18 U.S.C. § 1030(e)) can typically "sync" with a traditional desktop or laptop computer. The purpose of syncing a tablet to a traditional computer is to back up data that is stored on the tablet so that it is not permanently lost if the portable tablet is lost or damaged. Also, tablet users may move files off the tablet and onto a computer to free up storage space on the tablet. Similarly, computer (*e.g.*, desktop computers, tablets, etc.) users may move files off of one computer onto another computer or digital file storage devices such as a thumb drive, a DVD, an external hard drive to free up space on the computer. For this reason, I am seeking authorization to seize all computers and digital file storage devices reasonably believed to belong to or have been used by CRUZ in the **SUBJECT VEHICLE**—not any particular computer.

10. Finally, I know that many modern smart tablets, including Apple and Samsung-brand tablets, can be encrypted by the user using his finger and/or thumbprint or facial image to lock and unlock the device. Without the user's prints, the devices are difficult, if not impossible, for law enforcement personnel to unlock. Accordingly, I am requesting that, to the extent law enforcement seizes any tablet or smart cell phones or other computer described in Attachment B during a search of the **SUBJECT VEHICLE** (described in Attachment A), and if such device(s) features such encryption, then law enforcement may, while executing the search warrant of the **SUBJECT VEHICLE**, use

CRUZ's finger and/or thumbprint and/or facial image with any such encryption feature to attempt to unlock the device.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO POSSESS AND/OR ATTEMPT TO VIEW CHILD PORNOGRAPHY

11. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who possess and/or attempt to view child pornography:

a. Such individuals often receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals may possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines,

negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children often retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely completely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses,

telephone numbers, and usernames of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if CRUZ or other co-conspirators use a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the **SUBJECT VEHICLE**, or on his person as set forth in Attachment A.

STATEMENT OF PROBABLE CAUSE

12. On or about April 5, 2024, Sergeant Spencer Sloan of the Moore Police Department ("MPD") was dispatched to 2816 Yorkshire Drive in Moore, Oklahoma, in the Western District of Oklahoma. A Moore resident, T.L., was reporting someone peeking into her thirteen-year-old daughter's ("Jane Doe") window.

13. Upon his arrival, Sgt. Sloan deployed the department's drone that utilizes thermal imaging to survey the area for any possible suspects. Almost immediately, Sgt. Sloan located a heat signature in the backyard of 2813 Yorkshire Circle. Sgt. Sloan informed officers of his findings, and the subject began to move to the west. The subject continued westbound in the creek and hopped a fence into a backyard of a residence (2824 Kings Road). The subject then hopped into the backyard of 2820 Kings Road and then walked from the backyard to the front of the residence. The subject walked north until he was apprehended in front of 2824 Kings Rd. This was all recorded via the drone. MPD

Officer Koalton R. Keller asked the subject to identify himself. The subject lied about his name and date of birth. Ultimately, the subject was identified as CRUZ.

14. Sgt. Sloan then made his way to T.L.'s residence and spoke to T.L. According to T.L., she confiscated Jane Doe's laptop. T.L. allowed Sgt. Sloan to view the laptop where he observed messages between Jane Doe ("T" on discord) and "Alex." The conversation contained a few days' worth of messages. Several messages were sexual in nature. Jane Doe sent a photo to "Alex" depicting her vaginal area with the vagina covered with a hand. Sgt. Sloan confirmed the picture was sent by Jane Doe due to the red lights in the background that Jane Doe had in her room. Some of the messages were from "Alex" stating he wanted to use Jane Doe "like a toy.

15. MPD Detective Ryan Minard spoke to T.L., who advised the laptop belonged to Jane Doe's father S.P. who lived at another residence. Contact was made with the father, who consented to a search of the laptop.

16. Detective Minard observed on the discord app, on the laptop, that CRUZ was going by "Alex <3" as his username and Jane Doe was going by "T" as her username. CRUZ and Jane Doe communicated back and forth for several days. CRUZ made statements to Jane Doe about videos and pictures and how he knows Jane Doe has sent pictures to other people online. Jane Doe sent CRUZ a photograph of her while nude from the waist down. Cruz asked Jane Doe to face the camera and spread her legs for him. CRUZ asked Jane Doe to call on discord and they had multiple conversations through discord.

17. Cruz and Temperance met online using an application called "Discord" to communicate. Bryan advised Temperance that he went to Southmoore and Temperance

stated she was completing online school. During the conversation, Cruz asked Temperance how old she was, and she stated she was 13 years old about to turn 14. Cruz advised back that her age was okay in the conversation.

18. CRUZ told Jane Doe he wanted to "smash"[1] and asked how they could meet up. Jane Doe also expressed a desire to run away. Jane Doe talked about the cameras that were at her dads' house and how mother had less cameras. Jane Doe also advised her older brother turned the cameras around at her mom's house.

19. CRUZ told Jane Doe that they could meet up outside of her residence. CRUZ then talked about how he can't wait to be inside Jane Doe and for her body to take the shape of his. CRUZ then talked about making plans to sneak into Jane Doe's window when her mother goes to sleep.

20. On April 6, 2024, CRUZ drove the **SUBJECT VEHICLE** from Texas to Jane Doe's residence. CRUZ asked Jane Doe when to come to the house. The two talked back and forth waiting for T.L. to go to bed. CRUZ asked Jane Doe which window was her window so not to go to the wrong one. In the chat, Jane Doe told CRUZ to come back after running away from the window and that not to worry because Jane Doe's mother thought it was "Chris." At that point in the conversation, T.L. contacted police and the resulting response began.

21. Officer Koalton R. Keller found car keys in CRUZ's pockets. Officer Keller located a Toyota Sienna minivan at the intersection of NW 27th St/Yorkshire Ave that

[1] Based on my training and experience, "smash" is a slang term meaning to have sex.

responds to the key fob Officer Keller located. The vehicle was taken to Moore Police Department for evidence processing and secured at the Times Up Towing & Recovery LLC. At 208 Industrial Blvd. Moore, OK 73160.

22. CRUZ was interviewed by Detective Minard. After his interview, CRUZ asked Detective Minard if he would be allowed to make any phone calls. Detective Minard stated CRUZ would be allowed to make phone calls if he could remember their phone numbers, to which CRUZ stated he could not. Detective Minard asked CRUZ for consent to open CRUZ's phone but not go through it to help CRUZ get phone numbers out of the phone. CRUZ agreed by stating, "yes." CRUZ also provided the passcode to the phone, when asked.

23. On April 10, 2024, Detective Minard spoke to M.E., who identified herself as CRUZ's wife. She stated that they lived at 3524 Marwick Drive, Plano, Texas. She also informed Detective Minard that CRUZ had told her he was traveling to a friend's wedding in Texas.

24. Through the use of law enforcement databases, it was discovered that on September 10, 2020, Dropbox LLC self-reported user doe00084@gmail.com/ESP, User ID: 3196730080, for uploading 19 images/videos of child pornography. Three of the IP addresses associated with the CyberTip came back to Andrea Vilchis, CRUZ's girlfriend during that period of time. Six other IP addresses associated with the CyberTip were traced back to Jorge Alvarez, CRUZ's roommate during that period of time. The remaining two IP addresses were associated with Ruth Pina, CRUZ's mother. The resulting investigation did not lead to any criminal charges.

CONCLUSION

25. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that CRUZ committed the following crimes: Attempted Coercion and Enticement of a Minor, in violation of 18 U.S.C. § 2422(b); Interstate Travel with the Intent to Engage in a Sexual Act with a Minor, in violation of 18 U.S.C. § 2423(b); and Possession of Child Pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B).

26. Additionally, there is probable cause to believe that evidence of the criminal offenses is located in the **SUBJECT VEHICLE**, and this evidence, listed in Attachment B to this Affidavit, incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses. As described in the probable cause section, there is probable cause to believe CRUZ violated the aforementioned statutes. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

Andrea Salazar
Special Agent
Homeland Security Investigations

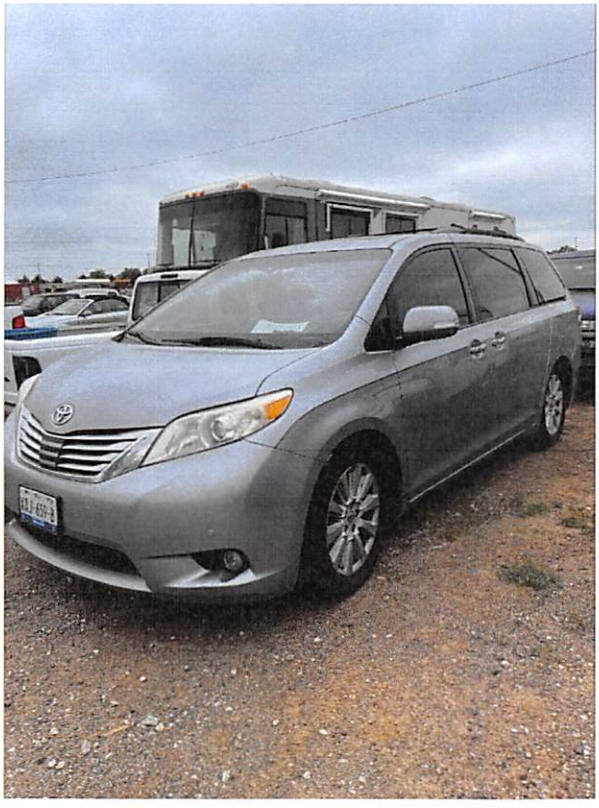
Sworn and subscribed before me this 22nd day of April, 2024.

SHON T. ERWIN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PROPERTY TO BE SEARCHED

This warrant seeks to search the Toyota Sienna, driven by CRUZ from Texas to Oklahoma, Serial Vin TDYK3DC6DS333454, with Tamaulipas, Mexico license plates XAJ-659-B ("**SUBJECT VEHICLE**"). The **SUBJECT VEHICLE** is currently secured at the Times Up Towing & Recovery LLC. at 208 Industrial Blvd. Moore, OK 73160, in the Western District of Oklahoma, and it is depicted below:



ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

Contraband, evidence, fruits, and instrumentalities related to CRUZ committing Attempted Coercion and Enticement of a Minor, in violation of 18 U.S.C. § 2422(b); Interstate Travel with the Intent to Engage in a Sexual Act with a Minor, in violation of 18 U.S.C. § 2423(b); and Possession of Child Pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B), in any form, including, but not limited to:

1. Computer(s), as broadly defined in 18 U.S.C. § 1030(e) and all other digital file storage devices, including (but not limited to) desktop computers, smart phones, e-readers, tablets, thumb drives, SD cards, DVDs, compact discs, and external hard drives; all computer hardware, computer software; computer related devices and documentation; computer passwords and data security devices; videotapes; video recording devices; video recording players; and video display monitors that may be, or are used to visually depict child pornography or child erotica, display or access information pertaining to a sexual interest in child pornography, display or access information pertaining to sexual activity with children, or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

2. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession,

receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

3. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.

4. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of the computer or by other means for the purpose of distributing or receiving child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

5. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8)

or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.

8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

9. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

11. Any and all cameras, film, videotapes or other photographic equipment capable of storing images or videos of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.

12. Any and all visual depictions of minors to see if they match images of minors in child pornography.

13. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

14. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership of the vehicle described above, including, but not limited to, rental or lease agreements, purchase documents, rental or lease payments, registration paperwork, mail envelopes, or addressed correspondence.

15. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

16. Any and all equipment associated with routers, modems, and network equipment used to connect computers to the Internet.

If a smart cell phone or other computer, as described herein, is found that requires access by using a finger or thumbprint or facial recognition to unlock the device, then, while executing the search warrant of the **SUBJECT VEHICLE**, a law enforcement officer may press the finger or thumbprint of Bryan Cruz onto the device to try to unlock it or use their face to unlock the device via facial recognition.